Collect. Math. **50**, 3 (1999), 243–267

Frobenius indices of certain curves over finite fields

Keisuke Toki

Kōyama 3-5-5, Nerima-ku, Tokyo 176-0022, Japan

Received November 11, 1997. Revised June 11, 1998

Abstract

We consider an algebraic curve $X \subset \mathbb{P}^N (N \geq 3)$ defined over a finite field of characteristic $p > 0$ which possesses an *order-sequence* in the sense of [6]. Let N, an odd prime number p and an integer $I (1 \leq I \leq N)$ be arbitrarily given. Then we shall give an example of a curve as above whose $q'-$*Frobenius index* in the sense of [1] equals I, which is a complete intersection in $\mathbb{P}^N$ of $N - I$ Fermat equations and $I - 1$ Artin-Schreier equations over a finite field $\mathbb{F}_{q'}$ with q' elements, where q' is some power of p (see the Theorem of Section 1). In the case of $N = 3$ and $I = 1$, our example is the same one as Example 3 in [1] or [2].

1. Introduction

Let $X \subset \mathbb{P}^N$ be an algebraic curve lying in an $N-$dimensional projective space $\mathbb{P}^N$ with $N \geq 3$ defined over a finite field $\mathbb{F}_{q'}$ of the given characteristic p, which possesses an *order-sequence* in the sense of [6].

In the present paper, we are concerned with the index, which is called the $q'-$*Frobenius index* in [1], of a certain order in the order-sequence, for a curve as above $X \subset \mathbb{P}^N$.

According to [1], notions of "*order-sequence*, $q'-$Frobenius *order-sequence* (resp. *index*)" will be as follows.

Let $x_0 : x_1 : x_2 : \cdots : x_N$ be the coordinate functions of $X \subset \mathbb{P}^N$, and $\{D^{(r)}; 0 \leq r \in \mathbb{Z}\}$ be the system of Hasse-Schmidt derivatives with respect to some separating variable on the curve X, where $\mathbb{Z}$ denotes the set of integers.

The *order-sequence* of the curve $X \subset \mathbb{P}^N$

$$0 = \varepsilon_0 < \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_N \tag{1.1}$$

means the minimal sequence consisting of integers, in the lexicographic order, such that the $N+1$ row-vectors $D^{(\varepsilon_i)} \cdot \mathfrak{x}(0 \le i \le N)$ are linearly independent over the function-field $k(X)$ of the curve X, where

$$\begin{aligned} \mathfrak{x} &= (x_0, x_1, x_2, \ldots, x_N), \\ D^{(\varepsilon_i)} \cdot \mathfrak{x} &= \big(D^{(\varepsilon_i)}(x_0),\, D^{(\varepsilon_i)}(x_1),\, D^{(\varepsilon_i)}(x_2), \ldots, D^{(\varepsilon_i)}(x_N)\big);\ 0 \le i \le N. \end{aligned}$$

And the $q'-$*Frobenius order-sequence* of the curve $X \subset \mathbb{P}^N$

$$0 = \nu_0 < \nu_1 < \nu_2 < \cdots < \nu_{N-1} \tag{1.2}$$

means the minimal sequence consisting of integers, in the lexicographic order, such that the $N+1$ row-vectors $\mathfrak{x}^{q'}, D^{(\nu_i)} \cdot \mathfrak{x}(0 \le i \le N-1)$ are linearly independent over $k(X)$, where

$$\begin{aligned} \mathfrak{x}^{q'} &= \big(x_0^{q'}, x_1^{q'}, x_2^{q'}, \ldots, x_N^{q'}\big), \\ D^{(\nu_i)} \cdot \mathfrak{x} &= \big(D^{(\nu_i)}(x_0), D^{(\nu_i)}(x_1), \ldots, D^{(\nu_i)}(x_N)\big); 0 \le i \le N-1\,. \end{aligned}$$

For the relationship between (1.1) and (1.2), it is known that there exists an integer I depending on q', with $1 \le I \le N$, such that

$$\nu_i = \begin{cases} \varepsilon_i & \text{whenever} \quad i < I \\ \varepsilon_{i+1} & \text{whenever} \quad i \ge I \end{cases} \tag{1.3}$$

(cf. Proposition 2.1 in [6]).

Hereafter, for the given curve $X \subset \mathbb{P}^N$ as above, we put

$$\iota(q'; X) := \text{the integer} \quad I \quad \text{as in (1.3).}$$

Then $\iota(q'; X)$ is called the $q'-$*Frobenius index* of the curve $X \subset \mathbb{P}^N$. For example, we know the following:

(a) Example 3 in [1] or [2] satisfies $\iota(q'; X) = 1$ for some q' (a curve which is a complete intersection of Fermat equations, in $N = 3$),

(b) The monomial curve in Theorem 3 of [1] satisfies $\iota(q'; X) = N$ for any q', any N (a curve which is an image of $\mathbb{P}^1$),

(c) Example 9 in [1] satisfies $\iota(q'; X) = N - 1$ for some q', any N (a curve which is an image of $\mathbb{P}^1$).

Now, let an integer $N \geq 3$ and an odd prime number p be arbitrarily given. We take arbitrarily an integer I with $1 \leq I \leq N$. Then it is our object to give an example of $X \subset \mathbb{P}^N$ over $\mathbb{F}_{q'}$ satisfying $\iota(q'; X) = I$, which is a complete intersection in $\mathbb{P}^N$, where q' is some power of p. Precisely speaking, our result is as follows:

Theorem

Let the triplet $\{N, p, I\}$ as above be given. We consider the following cases [A], [B], [C].

[A] Case $I = 1$.

Let a positive integer e satisfy $N \leq p^e$. Let p_i's $(1 \leq i \leq N-2)$ be elements in $\mathbb{F}_q$ such that "$p_i \neq 0, 1$ for each i" and "$p_i \neq p_j$ for $i \neq j$". We put

$$x = \frac{x_1}{x_0}, y = \frac{x_2}{x_0}, z_i = \frac{x_{i+2}}{x_0}(1 \leq i \leq N-2)\,.$$

We consider the curve X in $\mathbb{P}^N$ defined by $N-1$ Fermat equations over $\mathbb{F}_q$:

$$x^{q+1} + y^{q+1} = 1,\; x^{q+1} + z_i^{q+1} = p_i(1 \leq i \leq N-2)\,,$$

where $q = p^e$.

[B] Case $I = N$.

Let a positive integer e satisfy $N \leq p^e$. We take the sequence of successively increasing integers

$$2 = m_1 < m_2 < m_3 < \cdots, \quad \text{where} \quad m_i \not\equiv 0 \pmod{p}$$

for $i \geq 1$. We put

$$x = \frac{x_1}{x_0}, u_i = \frac{x_{i+1}}{x_0}(1 \leq i \leq N-1)\,.$$

(B_1); $I \leq p^e - p^{e-1} + 1$ Case. We consider the curve X in $\mathbb{P}^N$ defined by $N-1$ Artin-Schreier equations over $\mathbb{F}_q$:

$$u_i^q + u_i = x^{m_i}(1 \leq i \leq N-2), u_{N-1}^{q^2} + u_{N-1} = x^{q^2+1}\,,$$

where $q = p^e$.

(B_2); $I > p^e - p^{e-1} + 1$ Case. We consider the curve X in $\mathbb{P}^N$ defined by $N-1$ Artin-Schreier equations over $\mathbb{F}_q$:

$$u_i^q + u_i = x^{m_i}(1 \leq i \leq p^e - p^{e-1} - 1)\,,$$
$$u_{p^e - p^{e-1}+i}^{q^{i+2}} + u_{p^e-p^{e-1}+i} = x^{q^{i+2}+1}(0 \leq i \leq N - p^e + p^{e-1} - 1)\,,$$

where $q = p^e$.

[C] Case $1 < I < N$.

Let a positive integer e_0 *satisfy* $e_0 > 1$ *and* $N \le p^{e_0} - p^{e_0-1} + 1$. *We put*

$$x = \frac{x_1}{x_0}, y = \frac{x_2}{x_0}, z_i = \frac{x_{i+2}}{x_0}(1 \le i \le N - I - 1)\,,$$
$$u_j = \frac{x_{N-I+j+1}}{x_0}(1 \le j \le I - 1)\,.$$

We consider the curve X *in* $\mathbb{P}^N$ *defined by* $N - I$ *Fermat equations and* $I - 1$ *Artin-Schreier equations over* $\mathbb{F}_{q_0}$*:*

$$x^{q_0+1} + y^{q_0+1} = 1, x^{q_0+1} + z_i^{q_0+1} = p_i(1 \le i \le N - I - 1)\,,$$
$$u_j^{q_0} + u_j = x^{m_j}(1 \le j \le I - 1)\,,$$

where $q_0 = p^{e_0}$, *the* p_i*'s being elements in* $\mathbb{F}_{q_0}$ *such that "*$p_i \ne 0, 1$ *for each* i*" and "*$p_i \ne p_j$ *for* $i \ne j$*", the* m_j*'s being as in [B].*

Then, in each of the cases [A], [B], [C], the curve $X \subset \mathbb{P}^N$ *possesses the order-sequence, and it is obtained that*

$$\iota(q'; X) = I \quad if \quad q' = q^2, \quad in\ Cases\ [A], [B]$$
$$\iota(q'; X) = I \quad if \quad q' = q_0^2, \quad in\ Case\ [C]\,.$$

Note. The author is thankful to Mr. Takasi Masuda who has indicated the choice for "p_i's" in the Theorem.

The above cited example (a) has become a hint of this theorem. In order to prove the Theorem, we need to find the order-sequence of $X \subset \mathbb{P}^N$ in each of the cases [A], [B], [C]. For the sake of it, we shall use the "Hasse-Schmidt derivatives with respect to x", which are denoted by "$D_x^{(r)}; 0 \le r \in \mathbb{Z}$". We use the following known properties:

(1.4) $$D_x^{(0)} = id., D_x^{(r)}(c) = 0 \quad \text{for any constant} \quad c(r \ge 1)\,,$$
$$D_x^{(r)}(x^m) = \binom{m}{r} x^{m-r} \quad \text{for} \quad 0 < m \in \mathbb{Z}\,,$$

where $\binom{m}{r}$ is the binomial coefficient,

$$D_x^{(r)}\big(D_x^{(r')}(h)\big) = \binom{r + r'}{r'} D_x^{(r+r')}(h)\,,$$
$$D_x^{(r)}(g + h) = D_x^{(r)}(g) + D_x^{(r)}(h)\,,$$
$$D_x^{(r)}(g \cdot h) = \sum_{i=0}^{r} D_x^{(i)}(g) D_x^{(r-i)}(h)\,,$$
$$D_x^{(r)}(h^{q'}) = \begin{cases} \big(D_x^{(r/q')}(h)\big)^{q'} & \text{if} \quad r \equiv 0 \pmod{q'}\,, \\ 0 & \text{if} \quad r \not\equiv 0 \pmod{q'}\,, \end{cases}$$

for any functions g, h on the curve X (cf. [2], [4], [6]).

Moreover, for the congruence modulo a prime number p of the binomial coefficient $\binom{\alpha}{\beta}$ with $0 \leq \alpha, \beta \in \mathbb{Z}$, we use the following known property:

$$\binom{\alpha}{\beta} \equiv \prod_{i=0}^{n} \binom{a_i}{b_i} \mod p\,, \tag{1.5}$$

where $\alpha = \sum_{i=0}^{n} a_i p^i$, $\beta = \sum_{i=0}^{n} b_i p^i$, $0 \leq a_i, b_i \leq p-1 (0 \leq i \leq n)$ in $\mathbb{Z}$.

In Section 2, we shall find the order-sequence of the curve $X \subset \mathbb{P}^N$ in the Theorem, through direct computation.

In Section 3, we shall give a proof of the Theorem. In both Sections 2, 3, the formulas (1.4), (1.5) will be chiefly useful.

In Section 4, we shall apply the estimation-formula on the number of rational points on curves, which has been given in [3], to the curve of Case [A] in the Theorem, and show the number itself.

The author wishes to express his hearty thanks to Professor M. Homma who has told him about notions and known-facts on the "order-sequences, q'−Frobenius order-sequences" of space curves.

2. The order-sequences

In this section, we shall find the sequence (1.1) for the curve $X \subset \mathbb{P}^N$ in the Theorem.

We put $\xi_i = \frac{x_i}{x_0} (0 \leq i \leq N)$ and

$$\mathfrak{f} := \left(\xi_0, \xi_1, \xi_2, \ldots, \xi_N\right).$$

Then two row-vectors $D_x^{(0)} \cdot \mathfrak{f}, D_x^{(1)} \cdot \mathfrak{f}$ are obviously linearly independent over $k(X)$.

To find the sequence (1.1) is to find the minimal one in the lexicographic order such that $N+1$ row-vectors $D_x^{(\varepsilon_i)} \cdot \mathfrak{f} (0 \leq i \leq N)$ are linearly independent over $k(X)$ (cf. Proposition 1.4 in [6]).

Now, we shall carry out this procedure, in each of the cases [A], [B], [C] in the Theorem.

Case [A].

By using (1.4) and (1.5), we obtain the following:

$$D_x^{(1)}(y) = (-1)\frac{x^q}{y^q}\,,\ D_x^{(1)}(z_i) = (-1)\frac{x^q}{z_i^q}\ (1 \leq i \leq N-2)\,; \tag{2.1}$$

(2.2) $$D_x^{(r)}(y) = D_x^{(r)}(z_i) = 0 \ (2 \le r \le q-1,\ 1 \le i \le N-2)\,;$$

(2.3) $$D_x^{(q)}(y) = \frac{x^{q^2} - x}{y^q(1 - x^{q^2+q})}\,,$$
$$D_x^{(q)}(z_i) = \frac{p_i(x^{q^2} - x)}{z_i^q(p_i - x^{q^2+q})}\,(1 \le i \le N-2)\,;$$

(2.4) $$D_x^{(q+1)}(y) = \frac{(-1)}{y^q(1 - x^{q^2+q})}\,,$$
$$D_x^{(q+1)}(z_i) = \frac{(-p_i)}{z_i^q(p_i - x^{q^2+q})}\,(1 \le i \le N-2)\,;$$

(2.5) $$D_x^{(q)}(y) \cdot D_x^{(q+1)}(z_i) = D_x^{(q)}(z_i) \cdot D_x^{(q+1)}(y)\,(1 \le i \le N-2)\,;$$

(2.6) $$D_x^{(q+j)}(y) = D_x^{(q+j)}(z_i) = 0\,(2 \le j \le q-1,\ 1 \le i \le N-2)\,;$$

(2.7) $$\begin{aligned} D_x^{(nq)}(y) &= \frac{(-1)}{y^q}\big(D_x^{(1)}(y)\big)^q \cdot D_x^{((n-1)q)}(y) \\ &= \frac{x^{nq^2} - x^{(n-1)q^2+1}}{y^q(1 - x^{q^2+q})^n}\,, \\ D_x^{(nq)}(z_i) &= \frac{(-1)}{z_i^q}\big(D_x^{(1)}(z_i)\big)^q \cdot D_x^{((n-1)q)}(z_i) \\ &= \frac{p_i(x^{nq^2} - x^{(n-1)q^2+1})}{z_i^q(p_i - x^{q^2+q})^n} \\ &\quad \big(2 \le n \le N-2(n \in \mathbb{Z}),\ 1 \le i \le N-2\big)\,; \end{aligned}$$

(2.8) $$\begin{aligned} D_x^{(nq+1)}(y) &= \frac{(-1)}{y^q}\big(D_x^{(1)}(y)\big)^q \cdot D_x^{((n-1)q+1)}(y)\,, \\ D_x^{(nq+1)}(z_i) &= \frac{(-1)}{z_i^q}\big(D_x^{(1)}(z_i)\big)^q \cdot D^{((n-1)q+1)}(z_i) \\ &\quad \big(2 \le n \le N-2(n \in \mathbb{Z}),\ 1 \le i \le N-2\big)\,; \end{aligned}$$

$$D_x^{(nq)}(y)\cdot D_x^{(nq+1)}(z_i)=D_x^{(nq)}(z_i)\cdot D_x^{(nq+1)}(y) \quad \big(2\le n\le N-2(n\in\mathbb{Z}),\, 1\le i\le N-2\big)\,; \tag{2.9}$$

$$D_x^{(nq+j)}(y)=D_x^{(nq+j)}(z_i)=0 \quad \big(2\le n\le N-2(n\in\mathbb{Z}),\, 2\le j\le q-1,\, 1\le i\le N-2\big)\,; \tag{2.10}$$

$$\begin{aligned} D_x^{((N-1)q)}(y)&=\frac{x^{(N-1)q^2}-x^{(N-2)q^2+1}}{y^q(1-x^{q^2+q})^{N-1}}\,,\\ D_x^{((N-1)q)}(z_i)&=\frac{p_i(x^{(N-1)q^2}-x^{(N-2)q^2+1})}{z_i^q(p_i-x^{q^2+q})^{N-1}}\\ &\quad (1\le i\le N-2)\,. \end{aligned} \tag{2.11}$$

By (2.5), (2.9), the following assertion

(2.12) “$D_x^{(sq)}\cdot\mathfrak{f}$, $D_x^{(sq+1)}\cdot\mathfrak{f}$ *are linearly dependent over* $k(X)$, *for* $1\le s\le N-2(s\in\mathbb{Z})$”

is true. Moreover, from (2.2), (2.6), (2.10), we get, for $s,t\in\mathbb{Z}$,

$$D_x^{(sq+t)}\cdot\mathfrak{f}=0 \quad \text{if} \quad 0\le s\le N-2,\ 2\le t\le q-1\,. \tag{2.13}$$

In addition to (2.12) and (2.13), it will be shown that the following assertion

(2.14) “$N+1$ *row-vectors* $D_x^{(0)}\cdot\mathfrak{f}$, $D_x^{(1)}\cdot\mathfrak{f}, D_x^{(sq)}\cdot\mathfrak{f}\,\big(1\le s\le N-1(s\in\mathbb{Z})\big)$ *are linearly independent over* $k(X)$” is true.

By (2.12), (2.13), (2.14), the set of linearly independent vectors in (2.14) becomes the minimal one in the lexicographic order.

¿From now, we shall show the truth of the assertion (2.14).

For $1\le m\le N-1$, we get $\mathfrak{g}_m=(y,z_1,z_2,\dots,z_{m-1})$ which is the row-vector with coordinates $y,z_i(1\le i\le m-1)$. Then we denote by Δ_m, the $m\times m-$matrix whose row vectors are m vectors $D_x^{(sq)}\cdot\mathfrak{g}_m(1\le s\le m)$. Then we have

$$\det\Delta_m=\begin{vmatrix} D_x^{(q)}(y) & D_x^{(q)}(z_1) & \cdots & D_x^{(q)}(z_{m-1})\\ D_x^{(2q)}(y) & D_x^{(2q)}(z_1) & \cdots & D_x^{(2q)}(z_{m-1})\\ \vdots & \vdots & \ddots & \vdots\\ D_x^{(mq)}(y) & D_x^{(mq)}(z_1) & \cdots & D_x^{(mq)}(z_{m-1}) \end{vmatrix} \tag{2.15}$$

and

$$\neq 0 \quad \text{in} \quad k(X), \qquad \text{for} \quad 1 \leq m \leq N-1\,.$$

In fact, through (2.3), (2.7), (2.11), we shall compute the determinant of (2.15). Then we get

$$\det \Delta_m = \frac{\prod_{i=1}^{m-1} p_i \prod_{j=1}^{m} (x^{jq^2} - x^{(j-1)q^2+1})}{(yz_1z_2\cdots z_{m-1})^q \{ \prod_{i=0}^{m-1} (p_i - x^{q^2+q}) \}^m} \cdot \Phi_m(x)\,, \tag{2.16}$$

$$\Phi_m(x) = \begin{vmatrix} \varphi_{11}(x) & \varphi_{12}(x) & \cdots & \varphi_{1m}(x) \\ \varphi_{21}(x) & \varphi_{22}(x) & \cdots & \varphi_{2m}(x) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{m1}(x) & \varphi_{m2}(x) & \cdots & \varphi_{mm}(x) \end{vmatrix}$$

where $p_0 = 1$ and $\varphi_{ij}(x) = (p_{j-1} - x^{q^2+q})^{m-i}$ for $1 \leq i, j \leq m$.

Moreover, by using the assumption for the p_i's, it is obtained that

$$\Phi_m(0) = \prod_{i=1}^{m-1} (1 - p_i) \cdot \prod_{1 \leq i < j \leq m-1} (p_i - p_j) \neq 0\,,$$

through computing the determinant-expression of $\Phi_m(0)$. Therefore the polynomial $\Phi_m(x)$ is an non-zero element in $\mathbb{F}_q[x]$. And then $\det \Delta_m \neq 0$ in $k(X)$, by (2.16) and the assumption for the p_i's.

On the other hand, when we consider the $(N+1) \times (N+1)-$matrix Δ (resp. $2 \times 2-$matrix Δ_0) whose row vectors are $N+1$ vectors in (2.14) (resp. two vectors $(1, x), (0, 1)$), we have

$$\det \Delta = \det \Delta_0 \cdot \det \Delta_{N-1} \neq 0$$

by (2.15) and "$\det \Delta_0 = 1$".

Consequently, the truth of the assertion (2.14) has been shown. Thus *the order-sequence of the curve* $X \subset \mathbb{P}^N$ *in* Case [A] *is as follows*:

$$\varepsilon_0 = 0, \varepsilon_1 = 1, \varepsilon_{1+i} = iq(1 \leq i \leq N-1)\,.$$

Case [B].

First, we consider the case (B_1). We divide this case into the following subcases

$(B_1 - 1):$ $\quad I = N \leq 2p - 1\,,$

$(B_1 - \alpha):$ $\quad \alpha p - \alpha + 2 \leq I = N \leq \alpha p - \alpha + p\,,$ where

$$2 \leq \alpha \leq p^{e-1} - 1 (\alpha \in \mathbb{Z})\,.$$

Case $(B_1 - 1)$. In this case, we have

$$\text{if} \quad I \leq p \quad \text{then} \quad m_i = i + 1 (1 \leq i \leq I - 2)\,,$$
$$\text{if} \quad p < I \leq 2p - 1 \quad \text{then}$$
$$m_i = i + 1 (1 \leq i \leq p - 2),\, m_{p-2+i} = p + i (1 \leq i \leq N - p)\,.$$

We set, in case $I \leq p$, for $1 \leq i \leq I - 2\,,$

$$U_i = \begin{pmatrix} D_x^{(2)}(u_1) & D_x^{(2)}(u_2) & \cdots & D_x^{(2)}(u_i) \\ D_x^{(3)}(u_1) & D_x^{(3)}(u_2) & \cdots & D_x^{(3)}(u_i) \\ \vdots & \vdots & \ddots & \vdots \\ D_x^{(i+1)}(u_1) & D_x^{(i+1)}(u_2) & \cdots & D_x^{(i+1)}(u_i) \end{pmatrix}$$

and set, in case $p < I \leq 2p - 1$,

$$V_j = \begin{pmatrix} D_x^{(p)}(u_{p-1}) & D_x^{(p)}(u_p) & \cdots & D_x^{(p)}(u_{p-1+j}) \\ D_x^{(p+1)}(u_{p-1}) & D_x^{(p+1)}(u_p) & \cdots & D_x^{(p+1)}(u_{p-1+j}) \\ \vdots & \vdots & \ddots & \vdots \\ D_x^{(p+j)}(u_{p-1}) & D_x^{(p+j)}(u_p) & \cdots & D_x^{(p+j)}(u_{p-1+j}) \end{pmatrix}$$

for $0 \leq j \leq I - p - 1$.

Then the types of these matrices are as follows:

(2.17) *"U_i is of $i \times i-$triangular type with all 1 (resp. all 0) on the principal diagonal (resp. below the principal diagonal), and hence* $\det U_i \neq 0 (1 \leq i \leq I - 2)$".

(2.18) *"V_j is of $(j+1) \times (j+1)-$type with its transposal such that*

1*st-row:* $\left(\binom{1}{0}x,\, \binom{1}{1},\, 0, 0, \ldots, 0\right),$

2nd-row: $\left(\binom{2}{0}x^2,\ \binom{2}{1}x,\ \binom{2}{2},\ 0,\ldots,0\right)$,

....

j*th-row*: $\left(\binom{j}{0}x^j,\ \binom{j}{1}x^{j-1},\ \binom{j}{2}x^{j-2},\cdots,\binom{j}{j-1}x,\ \binom{j}{j}\right)$,

(j+1)*th-row*: $\left(\binom{j+1}{0}x^{j+1},\ \binom{j+1}{1}x^j,\ \binom{j+1}{2}x^{j-1},\ldots,\binom{j+1}{j}x\right)$,

and hence it is verified that $\det V_j \neq 0\ (0 \le j \le I-p-1)$*".*

Now we shall verify the claim of "det . $\neq 0$" in (2.18). Consider the linear relation $\sum_{i=0}^{j}\lambda_i \mathfrak{u}_i = 0$ of the row-vectors $\mathfrak{u}_i (0 \le i \le j)$ of V_j over $k(X)$. Then we have

$$\lambda_1 = (-1)\lambda_0 x,\ \lambda_2 = (-1)^2\lambda_0 x^2,\ldots,\lambda_j = (-1)^j\lambda_0 x^j$$

and

$$\sum_{i=0}^{j}\binom{j+1}{i}\lambda_i x^{j+1-i} = 0\,.$$

Hence, from these equations, we get

$$(-1)^{j+2}\binom{j+1}{j+1}\lambda_0 x^{j+1} = \left(\sum_{i=0}^{j}(-1)^i\binom{j+1}{i}\right)\lambda_0 x^{j+1} = 0\,.$$

Therefore $\lambda_0 = 0$ and hence $\lambda_i = 0 (0 \le i \le j)$. Then the $\mathfrak{u}_i$'s$(0 \le i \le j)$ are linearly independent over $k(X)$ and hence $\det V_j \neq 0 (0 \le j \le p-2)$.

Let M_h be the $h \times (N+1)-$matrix whose row vectors are h vectors $D_x^{(i)} \cdot \mathfrak{f}(0 \le i \le h-1)$. Then it is easily seen that some $I-$minor of M_I equals

$$\det\Delta_0 \cdot \det U_{I-2} \quad \text{if} \quad I \le p\,,$$
$$\det\Delta_0 \cdot \det U_{p-2} \cdot \det V_{I-p-1} \quad \text{if} \quad p < I \le 2p-1\,.$$

Hence, by "$\det\Delta_0 = 1$", (2.17), (2.18), the following assertion

(2.19) "*I row-vectors $D_x^{(i)} \cdot \mathfrak{f}(0 \le i \le I-1)$ are linearly independent over $k(X)$*"

is true.

For $I \le j \le q^2-1$, let $M_{I,j}$ be the matrix whose row vectors are $I+1$ vectors $D_x^{(i)} \cdot \mathfrak{f}(0 \le i \le I-1)$, $D_x^{(j)} \cdot \mathfrak{f}$. Then $M_{I,j}$ is a square matrix by $I = N$, and it is also easily seen that

(2.20) "$\det M_{I,j} = 0$ *for* $I \le j \le q^2-1$, *and hence these* $N+1$ *row-vectors are linearly dependent over k(X)*".

On the other hand, for $j = q^2$, we have

$$\det M_{I,q^2} = \det \Delta_0 \cdot \det U_{I-2} \cdot \det V_{I-p-1} \cdot (x - x^{q^4}),$$

because the transposed $(I+1)-$th column vector of M_{I,q^2} equals

$$\big(u_{I-1}, x^{q^2}, 0, 0, \ldots, 0, x - x^{q^4}).$$

Since the left-hand side of this equality is not zero by "$\det \Delta_0 = 1$", (2.17), (2.18), we obtain the truth of the following assertion

(2.21) "$N+1$ *row-vectors* $D_x^{(i)} \cdot \mathfrak{f}(0 \le i \le N-1), D_x^{(q^2)} \cdot \mathfrak{f}$ *are linearly independent over* $k(X)$".

By (2.19), (2.20), (2.21), the set of $N+1$ row-vectors in (2.21) becomes the minimal one in the lexicographic order. Thus *the order-sequence of the curve* $X \subset \mathbb{P}^N$ *in* Case $(B_1 - 1)$ *is as follows*:

$$\varepsilon_i = i(0 \le i \le N-1),\ \varepsilon_N = q^2.$$

Case $(B_1 - \alpha)$. In this case, at each α, we have, for $r \in \mathbb{Z}$,

$$\begin{aligned} m_i &= i + 1 \quad (1 \le i \le p-2), \\ m_{rp-r-1+i} &= rp + i \quad (1 \le i \le p-2,\ 1 \le r \le \alpha - 1), \\ m_{\alpha p - \alpha - 1 + i} &= \alpha p + i \quad (1 \le i \le I - 1 + \alpha - \alpha p). \end{aligned}$$

We set, for $0 \le j \le p-2$, $0 < s, r \le \alpha$,

$$U_j^{(s)} = \begin{pmatrix} u_{11}^{(s)} & u_{12}^{(s)} & \cdots & u_{1p-2}^{(s)} \\ u_{21}^{(s)} & u_{22}^{(s)} & \cdots & u_{2p-2}^{(s)} \\ \vdots & \vdots & \ddots & \vdots \\ u_{j+11}^{(s)} & u_{j+12}^{(s)} & \cdots & u_{j+1p-2}^{(s)} \end{pmatrix}$$

where $u_{i'j'}^{(s)} = D_x^{(sp+i'-1)}(u_{j'})$ for $1 \le i' \le j+1$, $1 \le j' \le p-2$,

$$V_{p-2,j} = \begin{pmatrix} v_{11}^{(1)} & v_{12}^{(1)} & \cdots & v_{1j+1}^{(1)} \\ v_{21}^{(1)} & v_{22}^{(1)} & \cdots & v_{2j+1}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ v_{p-11}^{(1)} & v_{p-12}^{(1)} & \cdots & v_{p-1j+1}^{(1)} \end{pmatrix}$$

where $v^{(1)}_{i'j'} = D_x^{(p+i'-1)}(u_{p-2+j'})$ for $1 \le i' \le p-1$, $1 \le j' \le j+1$,

$$V^{(s,r)}_{p-2,j} = \begin{pmatrix} v^{(s,r)}_{11} & v^{(s,r)}_{12} & \cdots & v^{(s,r)}_{1j+1} \\ v^{(s,r)}_{21} & v^{(s,r)}_{22} & \cdots & v^{(s,r)}_{2j+1} \\ \vdots & \vdots & \ddots & \vdots \\ v^{(s,r)}_{p-11} & v^{(s,r)}_{p-12} & \cdots & v^{(s,r)}_{p-1j+1} \end{pmatrix}$$

where $v^{(s,r)}_{i'j'} = D_x^{(sp+i'-1)}(u_{rp-r+j'-1})$ for $1 \le i' \le p-1$, $1 \le j' \le j+1$.

Then we have, for $0 \le j \le p-2$,

$$\begin{aligned} U^{(s)}_j &= 0,\ V^{(s,r)}_{p-2,j} = 0 (s > r)\,, \\ V^{(s,r)}_{p-2,j} &= \binom{r}{s} x^{(r-s)p} \cdot V_{p-2,j} \quad \text{for} \quad s \le r\,, \\ V^{(r,r)}_{p-2,p-2} &= V_{p-2,p-2} = V_{p-2} \quad \text{in case of} \quad s = r\,. \end{aligned} \tag{2.22}$$

It is seen that the following assertion

$(2.23)_1$ "*For $2p$ row-vectors $D_x^{(i)} \cdot \mathfrak{f} (0 \le i \le 2p-2)$, $D_x^{(j)} \cdot \mathfrak{f}$, these are linearly dependent ($j = 2p-1$), linearly independent ($j = 2p$) over $k(X)$*" is true.

In fact, in case $j = 2p-1$, we consider the linear relation

$$\sum_{i=0}^{2p-1} \lambda_i D_x^{(i)} \cdot \mathfrak{f} = 0 \quad \text{over} \quad k(X)\,.$$

Then, since $D_x^{(2p-1)} \cdot \mathfrak{f}$ equals the unit-vector with the $(2p-1)-$th coordinate 1, we have

$$\lambda_0 = \lambda_1 = \ldots = \lambda_{p-1} = 0,\ \lambda_{p+i} \in k(X) \cdot \lambda_p \quad (1 \le i \le p-1)$$

by (2.17), (2.18). Therefore $2p$ row-vectors as above are linearly dependent over $k(X)$. However, in case $j = 2p$, some $2p-$minor of the matrix M'_{2p} whose row vectors are $2p$ vectors as above equals

$$\det \Delta_0 \cdot \det U_{p-2} \cdot \det V_{p-2} \cdot x\,.$$

Therefore $2p$ row-vectors as above are linearly independent over $k(X)$, by "$\det \Delta_0 = 1$", (2.17), (2.18). Moreover we can show the truth of the following assertions at $r (2 \le r < \alpha), \alpha$:

$(2.23)_r$ "*For* $(r+1)p-r+1$ *row-vectors* $D_x^{(i)}\cdot\mathfrak{f}\,(0\le i\le 2p-2)$; $D_x^{(2p)}\cdot\mathfrak{f}$, $D_x^{(2p+i)}\cdot\mathfrak{f}$ $(1\le i\le p-2);\cdots;D_x^{(rp)}\cdot\mathfrak{f}$, $D_x^{(rp+i)}\cdot\mathfrak{f}(1\le i\le p-2)$; $D_x^{(j)}\cdot\mathfrak{f}$, *these are linearly dependent* $(j=(r+1)p-1)$, *linearly independent* $(j=(r+1)p)$ *over* $k(X)$" and

$(2.23)_\alpha$ "*For* $I+1$ *row-vectors* $D_x^{(i)}\cdot\mathfrak{f}(0\le i\le 2p-2)$; $D_x^{(2p)}\cdot\mathfrak{f}$, $D_x^{(2p+i)}\cdot\mathfrak{f}(1\le i\le p-2)$; $D_x^{(rp)}\cdot\mathfrak{f}$, $D_x^{(rp+i)}\cdot\mathfrak{f}(1\le i\le p-2, 2<r\le\alpha-1)$; $D_x^{(\alpha p)}\cdot\mathfrak{f}$, $D_x^{(\alpha p+i)}\cdot\mathfrak{f}(1\le i\le I+\alpha-2-\alpha p)$; $D_x^{(j)}\cdot\mathfrak{f}$, *these are linearly dependent* $(I+\alpha-1\le j\le q^2-1)$, *linearly independent* $(j=q^2)$ *over* $k(X)$".

In fact, in case $(2.23)_r$ with $j=(r+1)p-1$, we consider the linear relation over $k(X)$ of $(r+1)p-r+1$ row-vectors as above. Then, since $D_x^{((r+1)p-1)}\cdot\mathfrak{f}$ equals the unit-vectors with the $((r+1)p-r)-th$ coordinate 1, it is seen that these row-vectors are linearly dependent over $k(X)$. This is similar to the verification of "$(2.23)_1$ with $j=2p-1$". In case $(2.23)_r$ with $j=(r+1)p$, some $((r+1)p-r+1)-$minor of the matrix $M''_{(r+1)p-r+1}$ whose row vectors are $(r+1)p-r+1$ vectors as above equals

$$\det\Delta_0\cdot\det U_{p-2}\cdot\big(\det V_{p-2}\big)^r\cdot x\,.$$

Therefore these row-vectors are linearly independent over $k(X)$, by "$\det\Delta_0=1$", (2.17), (2.18).

In case $(2.23)_\alpha$ with $I+\alpha-1\le j\le q^2-1$, since $D_x^{(I+\alpha-1)}\cdot\mathfrak{f}$ equals the unit-vector with $I-$th coordinate 1 and each $D_x^{(I+\alpha-1+i)}\cdot\mathfrak{f}(1\le i\le q^2-1)$ equals the zero-vector, $I+1$ row-vectors as above are linearly dependent over $k(X)$. In case $(2.23)_\alpha$ with $j=q^2$, the square matrix M''_{I,q^2} whose row vectors are $I+1$ vectors as above satisfies that $\det M''_{I,q^2}$ equals

$$\det\Delta_0\cdot\det U_{p-2}\cdot\big(\det V_{p-2}\big)^{\alpha-1}\cdot\det V_{I-\alpha p+\alpha-2}\cdot(x-x^{q^4})\,.$$

Therefore $I+1$ row-vectors as above are linearly independent over $k(X)$, by "$\det\Delta_0=1$", (2.17), (2.18).

By $(2.23)_1$, $(2.23)_r$, $(2.23)_\alpha$, the set of $N+1$ row-vectors in $(2.23)_\alpha$ becomes the minimal one in the lexicographic order. Thus *the order-sequence of the curve* $X\subset\mathbb{P}^N$ *in* Case $(B_1-\alpha)$ *with* $2\le\alpha\le p^{e-1}-1$ *is as follows*:

$$\begin{aligned}\varepsilon_i&=i\qquad(0\le i\le 2p-2)\,,\\ \varepsilon_{rp-r+1+i}&=rp+i\quad(0\le i\le p-2, 2\le r\le\alpha-1)\,,\\ \varepsilon_{\alpha p-\alpha+1+i}&=\alpha p+i\quad(0\le i\le N-2+\alpha-\alpha p)\,,\\ \varepsilon_N&=q^2\,.\end{aligned}$$

Second, we consider the case (B_2). In this case, we have, for $r \in \mathbb{Z}$,

$$m_i = i + 1 \quad (1 \le i \le p-2)\,,$$
$$m_{rp-r-1+i} = rp + i \; (1 \le i \le p-1,\, 1 \le r \le p^{e-1} - 1)\,.$$

Let M''_{N+1} be the square matrix whose row vectors are $N+1$ vectors:

(2.24)
$$D_x^{(i)} \cdot \mathfrak{f} \quad (0 \le i \le 2p-2)\,,$$
$$D_x^{(rp)} \cdot \mathfrak{f},\, D_x^{(rp+i)} \cdot \mathfrak{f} \quad (1 \le i \le p-2,\, 2 \le r \le p^{e-1} - 1)\,,$$
$$D_x^{(q^i)} \cdot \mathfrak{f} \quad (2 \le i \le I - p^e + p^{e-1} + 1)\,.$$

Then we obtain

$$\det M''_{N+1} = \det \Delta_0 \cdot \det U_{p-2} \cdot \bigl(\det V_{p-2}\bigr)^{p^{e-1}-1} \times \prod_{i=2}^{I-p^e+p^{e-1}+1} (x - x^{q^{2i}})$$

by (2.22).

Hence, by (2.17), (2.18), we obtain the truth of the following assertion

(2.25) “$N+1$ *row-vectors in* (2.24) *are linearly independent over* $k(X)$”.

Moreover, we note that

(2.26) $$D_x^{(q^j+i)} \cdot \mathfrak{f} = 0 \quad \text{for} \quad 1 \le i < q^{j+1} - q^j, 2 \le j \le I - p^e + p^{e-1}\,.$$

Through the same argument as in the case (B_1), with considering (2.25), (2.26), the set of $N+1$ row-vectors in (2.24) becomes the minimal one in the lexicographic order. Thus *the order-sequence of the curve* $X \subset \mathbb{P}^N$ *in* Case (B_2) *is as follows*:

$$\varepsilon_i = i \quad (0 \le i \le 2p-2)\,,$$
$$\varepsilon_{rp-r+1+i} = rp + i \quad (0 \le i \le p-2,\, 2 \le r \le p^{e-1} - 1)\,,$$
$$\varepsilon_{p^e-p^{e-1}+1+i} = q^{i+2} \quad (0 \le i \le N - p^e + p^{e-1} - 2)\,,$$
$$\varepsilon_N = q^{N-p^e+p^{e-1}+1}\,.$$

Case [C].

At first, we note that "the $(p-2)\times(N-I)-$matrix whose row vectors are $p-2$ vectors $D_x^{(i)}\cdot\mathfrak{g}_{N-I}(2\le i\le p-1)$" and the "the $(j+1)\times(N-I)-$matrix whose row vectors are $j+1$ vectors $D_x^{(sp+i)}\cdot\mathfrak{g}_{N-I}(0\le i\le j)$ at each $\{j,s\}$ $(0\le j\le p-2,\ 1\le s\le p^{e_0-1}-1)$" are zero-matrices, by (2.2).

Let $\mathfrak{h}_r$ be the row-vector with coordinates $1, x, u_i(1\le i\le r-1)$ defined by

$$\mathfrak{h}_r=\big(1,x,u_1,u_2,\dots,u_{r-1}\big)\,.$$

(C_α) Let $\alpha p-\alpha+1\le I\le \alpha p-\alpha+p-1$, where

$$0\le\alpha\le p^{e_0-1}-1\ (\alpha\in\mathbb{Z}):$$

$\alpha=0$ Case. In this case, we have

$$m_i=i+1\ \ (1\le i\le I-1)\,.$$

Let H_r be the $(r+1)\times(r+1)-$matrix whose row vectors are $r+1$ vectors $D_x^{(i)}\cdot\mathfrak{h}_r(0\le i\le r)$. Then we have

$$\det H_I=\det\Delta_0\cdot\det U_{I-1}\,.$$

Hence the left-hand side of this equality is not zero. Therefore $I+1$ row-vectors $D_x^{(i)}\cdot\mathfrak{f}(0\le i\le I)$ are linearly independent over $k(X)$.

$\alpha=1$ Case. In this case, we have

$$m_i=i+1(1\le i\le p-2),\ m_{p-2+i}=p+i(1\le i\le I+1-p)$$

and

$$\det H_I=\det H_{p-1}\cdot\det V_{I-p}\,.$$

Therefore $I+1$ row-vectors $D_x^{(i)}\cdot\mathfrak{f}(0\le i\le I)$ are linearly independent over $k(X)$.

$\alpha=2$ Case. In this case, we have

$$\begin{aligned}m_i=i+1(1\le i\le p-2), m_{p-2+i}&=p+i(1\le i\le p-1)\,,\\ m_{2p-3+i}&=2p+i(1\le i\le I+2-2p)\,.\end{aligned}$$

By "$\alpha=1$ Case", the $2p-1$ row-vectors $D_x^{(i)}\cdot\mathfrak{f}(0\le i\le 2p-2)$ are linearly independent over $k(X)$. However it is seen that $2p$ row-vectors $D_x^{(i)}\cdot\mathfrak{f}(0\le i\le 2p-1)$ are linearly dependent over $k(X)$, by the same way as in $(2.23)_1$ with $j=2p-1$. And, for the $(I+1)\times(I+1)-$matrix $H_{I,I-2p+1}$ whose row vectors are $I+1$ vectors

$$D_x^{(i)}\cdot\mathfrak{h}_I(0\le i\le 2p-2),\ D_x^{(2p+i)}\cdot\mathfrak{h}_I(0\le i\le I-2p+1)\,,$$

we have

$$\det H_{I,I-2p+1} = \det H_{2p-2} \cdot \det V_{I-2p+1} \,.$$

Hence the left-hand side of this equality is not zero. Therefore $I+1$ row-vectors

$$D_x^{(i)} \cdot \mathfrak{f}(0 \le i \le 2p-2)\,,\ D_x^{(2p+i)} \cdot \mathfrak{f}(0 \le i \le I-2p+1)$$

are linearly independent over $k(X)$.

$\alpha \ge 3$ Case. In this case, we have, for $r \in \mathbb{Z}$,

$$\begin{aligned} m_i &= i+1 \quad (1 \le i \le p-2)\,, \\ m_{rp-r-1+i} &= rp+i \quad (1 \le i \le p-1,\ 1 \le r \le \alpha-1)\,, \\ m_{\alpha p-\alpha-1+i} &= \alpha p+i \quad (1 \le i \le I+\alpha-\alpha p)\,. \end{aligned}$$

Moreover it will be verified that $I+1$ row-vectors

$$\begin{gathered} D_x^{(i)} \cdot \mathfrak{f} \quad (0 \le i \le 2p-2)\,; \\ D_x^{(2p)} \cdot \mathfrak{f}, D_x^{(2p+i)} \cdot \mathfrak{f} \quad (1 \le i \le p-2)\,; \\ \cdots\cdots\cdots \\ D_x^{((\alpha-1)p)} \cdot \mathfrak{f}, D_x^{((\alpha-1)p+i)} \cdot \mathfrak{f} \quad (1 \le i \le p-2)\,; \\ D_x^{(\alpha p)} \cdot \mathfrak{f}, D_x^{(\alpha p+i)} \cdot \mathfrak{f} \quad (1 \le i \le I+\alpha-1-\alpha p) \end{gathered}$$

are linearly independent over $k(X)$ and the set of these $I+1$ row-vectors is the minimal one in the lexicographic order.

In $I+1$ row-vectors as above, we write $\mathfrak{h}_I$ for $\mathfrak{f}$ and denote by K_I, the $(I+1) \times (I+1)-$matrix whose row-vectors are these $I+1$ vectors. Then we note that

$$\det K_I = \det H_{p-1} \cdot \big(\det V_{p-2}\big)^{\alpha-1} \cdot \det V_{I+\alpha-1-\alpha p} \,.$$

¿From the defining-equation of the curve X, it is seen that

$$D_x^{(i)} \cdot \mathfrak{g}_{N-I} = 0 (2 \le i \le q_0-1),\ D_x^{(i)} \cdot \mathfrak{f} = 0 (I+\alpha+1 \le i \le q_0-1)\,.$$

We add $N-I$ row-vectors $D_x^{(jq_0)} \cdot \mathfrak{f}$ $(1 \le j \le N-I)$ to $I+1$ row-vectors as above. Let M be the $(N+1) \times (N+1)-$matrix whose row vectors are these $N+1$ vectors. Then we have

$$\det M = \pm \det \Delta_{N-I} \cdot \det K_I \,.$$

Through (2.5), (2.6), (2.9), (2.10), (2.22), the set of these $N+1$ row-vectors becomes the minimal one in the lexicographic order. Thus *the order-sequence of the curve*

$X \subset \mathbb{P}^N$ *in* Case [C] *is as follows*: In case $(C_\alpha); 0 \leq \alpha \leq p^{e_0-1}-1$, for $\alpha = 0, 1$ Case, we have

$$\varepsilon_i = i \ (0 \leq i \leq I), \quad \varepsilon_{I+i} = iq_0 \ (1 \leq i \leq N-I)\,.$$

for $\alpha \geq 2$ Case, we have

$$\begin{aligned} \varepsilon_i &= i \quad (0 \leq i \leq 2p-2)\,, \\ \varepsilon_{rp-r+1+i} &= rp+i \quad (0 \leq i \leq p-2,\ 2 \leq r \leq \alpha-1)\,, \\ \varepsilon_{\alpha p-\alpha+1+i} &= \alpha p+i \quad (0 \leq i \leq I-1+\alpha-\alpha p)\,, \\ \varepsilon_{I+i} &= iq_0 \quad (1 \leq i \leq N-I)\,. \end{aligned}$$

3. Proof of the Theorem

Let q' be a positive integer power of the characteristic p. By (1.3), in order to show "$\iota(q'; X) = I$", it is sufficient to show the truth of the following assertions:

(3.1) "$I+1$ *row-vectors* $\mathfrak{f}^{q'}$, $D_x^{(\varepsilon_i)} \cdot \mathfrak{f} (0 \leq i \leq I-1)$ *are linearly independent over* $k(X)$"

and

(3.2) "$I+2$ *row-vectors* $\mathfrak{f}^{q'}$, $D_x^{(\varepsilon_i)} \cdot \mathfrak{f} (0 \leq i \leq I)$ *are linearly dependent over* $k(X)$".

Case [A]. Let $q' = q^2$.

Since $x - x^{q'} \neq 0$, two row-vectors $\mathfrak{f}^{q'}, D_x^{(0)} \cdot \mathfrak{f}$ are linearly independent over $k(X)$. Then the assertion (3.1) is true.

Now we shall show the truth of the assertion (3.2). Let D_{ijk} with $i < j < k$, be the 3-minor consisting of the $i-$th column, the $j-$th column, the $k-$th column of $3 \times (N+1)-$matrix whose row vectors are three vectors $\mathfrak{f}^{q'}, D_x^{(0)} \cdot \mathfrak{f}, D_x^{(1)} \cdot \mathfrak{f}$. Then each D_{ijk} is as follows:

$$\begin{aligned}
D_{123} &= (x - x^{q'})D_x(y) - (y - y^{q'})\,,\\
D_{12k} &= (x - x^{q'})D_x(z_k) - (z_k - z_k^{q'})\,,\\
D_{13k} &= (y - y^{q'})D_x(z_k) - (z_k - z_k^{q'})D_x(y)\,,\\
D_{1kk'} &= (z_k - z_k^{q'})D_x(z_{k'}) - (z_{k'} - z_{k'}^{q'})D_x(z_k)\,,
\end{aligned}$$

$$\begin{aligned}
D_{23k} = \bigl(y^{q'} - x^{q'}D_x(y)\bigr)\bigl(z_k - xD_x(z_k)\bigr)\\
- \bigl(y - xD_x(y)\bigr)\bigl(z_k^{q'} - x^{q'}D_x(z_k)\bigr)\,,
\end{aligned}$$

$$\begin{aligned}
D_{2kk'} = \bigl(z_k^{q'} - x^{q'}D_x(z_k)\bigr)\bigl(z_{k'} - xD_x(z_{k'})\bigr)\\
- \bigl(z_k - xD_x(z_k)\bigr)\bigl(z_{k'}^{q'} - x^{q'}D_x(z_{k'})\bigr)\,,
\end{aligned}$$

$$\begin{aligned}
D_{3kk'} = {}&\bigl(z_k^{q'}z_{k'} - z_k z_{k'}^{q'}\bigr)D_x(y)\\
&- \bigl(y^{q'}z_{k'} - yz_{k'}^{q'}\bigr)D_x(z_k)\\
&+ \bigl(y^{q'}z_k - yz_k^{q'}\bigr)D_x(z_{k'})\,,
\end{aligned}$$

$$\begin{aligned}
D_{kk'k''} = {}&\bigl(z_{k'}^{q'}z_{k''} - z_{k'}z_{k''}^{q'}\bigr)D_x(z_k)\\
&- \bigl(z_k^{q'}z_{k''} - z_k z_{k''}^{q'}\bigr)D_x(z_{k'})\\
&+ \bigl(z_k^{q'}z_{k'} - z_k z_{k'}^{q'}\bigr)D_x(z_{k''})
\end{aligned}$$

$\bigl(D_x = D_x^{(1)},\ 4 \le k < k' < k''\bigr)$.

By using (2.1), we have, for $q' = q^2$,

$$\begin{aligned}
D_{123} &= \frac{-1}{y^q}\left\{1 - (x^{q+1} + y^{q+1})^q\right\},\\
D_{12k} &= \frac{-1}{z_k^q}\left\{(x^{q+1} + z_k^{q+1}) - (x^{q+1} + z_k^{q+1})^q\right\},\\
D_{13k} &= \frac{-x^q}{(yz_k)^q}\left\{(y^{q+1} - z_k^{q+1}) - (y^{q+1} - z_k^{q+1})^q\right\},\\
D_{1kk'} &= \frac{-x^q}{(z_k z_{k'})^q}\left\{(z_k^{q+1} - z_{k'}^{q+1}) - (z_k^{q+1} - z_{k'}^{q+1})^q\right\},
\end{aligned} \tag{3.3}$$

$$D_{23k} = \frac{1}{(yz_k)^q} \left\{ (x^{q+1} + y^{q+1})^q (x^{q+1} + z_k^{q+1}) \right. \\ \left. - (x^{q+1} + y^{q+1})(x^{q+1} + z_k^{q+1})^q \right\},$$

$$D_{2kk'} = \frac{1}{(z_k z_{k'})^q} \left\{ (x^{q+1} + z_k^{q+1})^q (x^{q+1} + z_{k'}^{q+1}) \right. \\ \left. - (x^{q+1} + z_k^{q+1})(x^{q+1} + z_{k'}^{q+1})^q \right\},$$

$$D_{3kk'} = \frac{-x^q}{(yz_k z_{k'})^q} \left\{ (z_k^{q+1} - y_k^{q+1})^q (z_{k'}^{q+1} - y^{q+1}) \right. \\ \left. - (z_k^{q+1} - y^{q+1})(z_{k'}^{q+1} - y^{q+1})^q \right\},$$

$$D_{kk'k''} = \frac{-x^q}{(z_k z_{k'} z_{k''})^q} \left\{ (z_{k'}^{q+1} - z_k^{q+1})^q (z_{k''}^{q+1} - z_k^{q+1}) \right. \\ \left. - (z_{k'}^{q+1} - z_k^{q+1})(z_{k''}^{q+1} - z_k^{q+1})^q \right\}.$$

Therefore, from the defining-equation of the curve, it is seen that these D_{ijk} are all vanished. Thus, for $q' = q^2$, three row-vectors $\mathfrak{f}^{q'}, D_x^{(0)} \cdot \mathfrak{f}$, $D_x^{(1)} \cdot \mathfrak{f}$ are linearly dependent over $k(X)$. Therefore the assertion (3.2) is true. Consequently, in Case [A], we have obtained

$$\iota(q'; X) = I \quad \text{if} \quad q' = q^2.$$

Case [B]. Let $q' = q^2$.

In this case, since $I = N$, the assertion (3.2) is true. Now we shall show the truth of the assertion (3.1), i.e., $\det M^{(q')} \neq 0$, where $M^{(q')}$ denotes the $(N+1) \times (N+1)-$matrix whose row vectors are $N+1$ vectors $\mathfrak{f}^{q'}, D_x^{(\varepsilon_i)} \cdot \mathfrak{f}(0 \leq i \leq N-1)$. We put

$$n := \begin{cases} 2 & \text{in Case} \quad (B_1) \\ N - p^e + p^{e-1} + 1 & \text{in Case} \quad (B_2), \end{cases}$$

$$\Delta^{(q')} := \begin{pmatrix} 1 & x^{q'} & u_{N-1}^{q'} \\ 1 & x & u_{N-1} \\ 0 & 1 & D_x(u_{N-1}) \end{pmatrix}.$$

By Section 2, it is seen that

$$D_x^{(\varepsilon_i)}(u_{N-1}) = 0 \quad \text{for} \quad 2 \leq i \leq N-1\,.$$

Then it is obtained that, in Case $(B_1 - 1)$;

$$\det M^{(q')} = \pm \det \Delta^{(q')} \cdot \det U_{I-2} \quad \text{if} \quad I \le p\,,$$
$$\det M^{(q')} = \pm \det \Delta^{(q')} \cdot \det U_{p-2} \cdot \det V_{I-p-1} \quad \text{if} \quad p < I \le 2p-1\,,$$

in Case $(B_1 - \alpha)$ for $2 \le \alpha \le p^{e-1}$;

$$\det M^{(q')} = \pm \det \Delta^{(q')} \cdot \det U_{p-2} \cdot \big(\det V_{p-2}\big)^{\alpha-1} \cdot \det V_{I-\alpha p+\alpha-2}\,,$$

in Case (B_2);

$$\det M^{(q')} = \pm \det \Delta^{(q')} \cdot \det U_{p-2} \cdot \big(\det V_{p-2}\big)^{p^{e-1}-1} \times \prod_{i=2}^{I-p^e+p^{e-1}} (x - x^{q^{2i}})\,.$$

By $D_x(u_{N-1}) = x^{q^n}$,

$$\det \Delta^{(q')} = (x - x^{q'})x^{q^n} - u_{N-1} + u_{N-1}^{q'}\,.$$

Therefore the left-hand side of this equality equals

$$2x^{q^2+1} - x^{2q^2} - 2u_{N-1} \quad \text{in Case} \quad (B_1)\,,$$
$$x^{q^n+1} - x^{q^2+q^n} - u_{N-1} + u_{N-1}^{q^2} \quad \text{in Case} \quad (B_2)$$

$(n = I - p^e + p^{e-1} + 1 \ge 3)$.

Hence $\det \Delta^{(q')} \ne 0$. Therefore, in Case [B], by (2.17), (2.18), we get $\det M^{(q')} \ne 0$. Consequently, in Case [B], we have obtained

$$\iota(q'; X) = I \quad \text{if} \quad q' = q^2.$$

Case [C]. Let $q' = q_0^2$.

Let $M_h^{(q')}$ be the $(h+2) \times (N+1)-$matrix whose row vectors are $h+2$ vectors $\mathfrak{f}^{q'}, D_x^{(\varepsilon_i)} \cdot \mathfrak{f}\,(0 \le i \le h)$.

In the matrix $M_I^{(q')}$, we take arbitrarily s vectors in the set of 1st-column, 2nd-column, 3rd-column,. . .,$(N - I + 2)$th-column vectors, and t vectors in the set of $(N - I + 3)$th-column, $(N - I + 4)$th-column,. . .,$(N + 1)$th-column vectors, where $s + t = I + 2$.

Then, since $s \geq 3$ by $0 \leq t \leq I-1$, s columns in the former set are linearly dependent over $k(X)$ by (3.3). Hence $s+t$ vectors as above are linearly dependent over $k(X)$. Therefore all $(I+2)-$minors of $M_I^{(q')}$ are vanished, and hence the assertion (3.2) is true.

Now we shall show the truth of the assertion (3.1). We put

$$S_I^{(q')} = M_I^{(q')} \begin{pmatrix} 1, 2, 3, \ldots, I+1 \\ 1, 2, N-I+3, \ldots, N+1 \end{pmatrix},$$

where the right-hand side denotes a $(I+1) \times (I+1)-$matrix whose row vectors (resp. column vectors) are 1st-row, 2nd-row, 3rd-row,$\ldots, (I+1)$th-row (resp. 1st-column, 2nd-column, $(N-I+3)$th-column,$\ldots, (N+1)$th-column) of $M_I^{(q')}$. Then we shall see that $\det S_I^{(q')} \neq 0$. Let S' be the $(I+1) \times (I+1)-$matrix obtained by subtracting 1st-row from 2nd-row in $S_I^{(q')}$, and let $T_I^{(q')}$ be the $I \times I-$matrix obtained by taking off 1st-row and 1st-column in S'. Then we have $\det S_I^{(q')} = \det T_I^{(q')}$. For our purpose, it is sufficient to show that $\det T_I^{(q')} \neq 0$. Now we put $T_I = T_I^{(q')}$.

Case $1 < I \leq p-1$:

The coordinates of 1st-row vector of T_I are $x - x^{q_0^2}, u_i - u_i^{q_0^2} (1 \leq i \leq I-1)$ respectively, and each $u_i - u_i^{q_0^2}$ equals $x^{i+1} - x^{(i+1)q_0} (1 \leq i \leq I-1)$. Since the determinant of $(I-1) \times (I-1)-$submatrix of T_I consisting of "i-th row, j-th column" elements $(2 \leq i \leq I, 1 \leq j \leq I-1)$ equals $\det U_{I-2}$, the set of 2nd-row, 3rd-row, 4th-row,$\ldots, I$ th-row vectors of T_I are linearly independent over $k(X)$, by (2.17).

Suppose that the 1st-row vector of T_I is a linear combination of these $I-1$ row-vectors with coefficients $\lambda_i (1 \leq i \leq I-1)$ in $k(X)$. Then we have

$$\lambda_1 = x - x^{q_0^2}, \lambda_i = (x^i - x^{iq_0}) - \sum_{j=1}^{i-1} \binom{i}{j} \lambda_j x^{i-j} (2 \leq i \leq I-1),$$

and moreover we have the equality

$$\sum_{i=1}^{I-1} \binom{I}{i} \lambda_i x^{I-i} = x^I - x^{Iq_0}.$$

The left-hand side of this equality is in $\mathbb{F}_p[x]$ and does not contain the term x^{Iq_0}. This is absurd. Thus we see that I row-vectors of T_I are linearly independent over $k(X)$. Hence we have $\det T_I \neq 0$.

Case $\alpha p - \alpha + 1 \leq I \leq \alpha p - \alpha + p - 1$, where

$$1 \leq \alpha \leq p^{e_0 - 1} - 1 \ (\alpha \in \mathbb{Z}):$$

The coordinates of 1st-row vector of T_I are $x - x^{q_0^2}, u_i - u_i^{q_0^2} (1 \leq i \leq p-2)$; $u_{p-2+i} - u_{p-2+i}^{q_0^2}; \ldots; u_{(\alpha-1)p-\alpha+i} - u_{(\alpha-1)p-\alpha+i}^{q_0^2} (1 \leq i \leq p-1)$; $u_{\alpha p-\alpha-1+i} - u_{\alpha p-\alpha-1+i}^{q_0^2} (1 \leq i \leq I + \alpha - \alpha p)$ respectively, and we have, by the defining-equation of the curve in Case [C],

$$\begin{aligned} u_i - u_i^{q_0^2} &= x^{i+1} - x^{(i+1)q_0} (1 \leq i \leq p-2)\,; \\ u_{p-2+i} - u_{p-2+i}^{q_0^2} &= x^{p+i} - x^{(p+i)q_0} (1 \leq i \leq p-1)\,; \\ &\cdots\cdots\cdots \\ u_{(\alpha-1)p-\alpha+i} - u_{(\alpha-1)p-\alpha+i}^{q_0^2} &= x^{(\alpha-1)p+i} - x^{((\alpha-1)p+i)q_0} (1 \leq i \leq p-1)\,; \\ u_{\alpha p-\alpha-1+i} - u_{\alpha p-\alpha-1+i}^{q_0^2} &= x^{\alpha p+i} - x^{(\alpha p+i)q_0} (1 \leq i \leq I + \alpha - \alpha p)\,. \end{aligned}$$

Since the determinant of $(I-1) \times (I-1)-$submatrix of T_I consisting of "i-th row, j-th column" elements $(2 \leq i \leq I,\ 1 \leq j \leq I-1)$ equals

$$\det U_{p-2} \cdot \big(\det V_{p-2}\big)^{\alpha-1} \cdot \det V_{I-2+\alpha-\alpha p}\,,$$

the set of 2nd-row, 3rd-row, 4th-row,..., Ith-row vectors of T_I are linearly independent over $k(X)$, by (2.17), (2.18). Suppose that the 1st-row vector of T_I is a linear combination of these $I-1$ row-vectors with coefficients $\lambda_i (1 \leq i \leq I-1)$ in $k(X)$.

"$\alpha = 1$ and $I = p$" Case. Then, in this case, we have

$$\lambda_1 = x - x^{q_0^2} \quad \text{and} \quad \binom{p+1}{1} \lambda_1 = x^{p+1} - x^{(p+1)q_0}\,.$$

Therefore $x^{q_0^2+p} = x^{(p+1)q_0}$. Since $q_0 = p^{e_0}$ with $e_0 > 1$, this is absurd. Thus we see that $\det T_I \neq 0$.

"$\alpha = 1$ and $I = p+1$" Case. Then, in this case, we have

$$\begin{aligned} &\lambda_1 = x - x^{q_0^2}\,,\ \lambda_2 = (x^2 - x^{2q_0}) - \binom{2}{1} \lambda_1 x, \\ &\binom{p+1}{1} \lambda_1 x^p + \binom{p+1}{p} \lambda_p x = x^{p+1} - x^{(p+1)q_0}, \\ &\binom{p+2}{1} \lambda_1 x^{p+1} + \binom{p+2}{2} \lambda_2 x^p + \binom{p+2}{p} \lambda_p x^2 = x^{p+2} - x^{(p+2)q_0}. \end{aligned}$$

The left-hand sides of these equalities are in $\mathbb{F}_p[x]$ and the left-hand side of the 4th equality does not contain the term $x^{(p+2)q_0}$. This is absurd. Thus we see that $\det T_I \neq 0$.

We shall proceed with the similar argument. Consequently, we shall obtain that $\det T_I \neq 0$ in each of the cases for $\{\alpha, I\}$.

Thus, in Case [C], we have obtained

$$\iota(q'; X) = I \quad \text{if} \quad q' = q_0^2.$$

4. The number of rational points in Case [A]

Let the curve $X \subset \mathbb{P}^N$ be as in Case [A] of the Theorem. First, we shall show that X is smooth. Expressing the equations defining this curve by the homogeneous forms, we have

$$\begin{aligned} h_0 &:= x_1^{q+1} + x_2^{q+1} - p_0 x_0^{q+1} = 0\,, \\ h_1 &:= x_1^{q+1} + x_3^{q+1} - p_1 x_0^{q+1} = 0\,, \\ h_2 &:= x_1^{q+1} + x_4^{q+1} - p_2 x_0^{q+1} = 0\,, \\ &\cdots\cdots \\ h_i &:= x_1^{q+1} + x_{i+2}^{q+1} - p_i x_0^{q+1} = 0\,, \\ &\cdots\cdots \\ h_{N-2} &:= x_1^{q+1} + x_N^{q+1} - p_{N-2} x_0^{q+1} = 0\,, \end{aligned}$$

$(p_0 = 1)$.

Then the Jacobian-matrix $J := \left(\frac{\partial h_i}{\partial x_j}\right)_{0 \le i \le N-2, 0 \le j \le N}$ of the curve $X \subset \mathbb{P}^N$ becomes

$$J = \begin{pmatrix} -p_0 x_0^q & x_1^q & x_2^q & 0 & 0 & \cdots & 0 \\ -p_1 x_0^q & x_1^q & 0 & x_3^q & 0 & \cdots & 0 \\ -p_2 x_0^q & x_1^q & 0 & 0 & x_4^q & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -P_{N-2} x_0^q & x_1^q & 0 & 0 & 0 & \cdots & x_N^q \end{pmatrix}.$$

Let the field k be an algebraic closure of $\mathbb{F}_q$. We shall verify that "rank $J = N-1$" at any point $P = (x_0 : x_1 : \cdots : x_N)$ in $X(k)$, as follows.

Suppose that rank $J < N-1$ at some point P in $X(k)$. Then, at P, there exists a linear relation $\sum_{i=0}^{N-2} \lambda_i \mathfrak{u}_i = 0$ of "row-vectors $\mathfrak{u}_i$'s in the matrix J", with coefficients λ_i in k, where some one of the λ_i's is not zero.

Now, suppose that $\lambda_i \neq 0$. Then $x_{i+2} = 0$ by $\lambda_i x_{i+2}^q = 0$. Moreover, suppose that there exist some $j(\neq i)$ such that $\lambda_j \neq 0$. Then, since $x_{i+2} = x_{j+2} = 0$, we have $p_i x_0^{q+1} = p_j x_0^{q+1}$ by $h_i(P) = h_j(P) = 0$. Hence $x_0 = 0$ by $p_i \neq p_j$. Therefore, assuming the existence of j as above, we get $x_0 = x_{i+2} = 0$ and hence $x_0 = x_1 = 0$ by $h_i(P) = 0$. Consequently, it occurs that "$x_0 = x_1 = x_r = 0$ for any r with $2 \leq r \leq N$", from "$h_s(P) = 0$ for any s with $0 \leq s \leq N-2$". This is absurd. Thus j as above does not exist. Then it occurs that if $\lambda_i \neq 0$ then $\lambda_j = 0$ for any $j(\neq i)$. And, in this case, we get $\lambda_i x_1^q = \lambda_i p_i x_0^q = 0$ and hence $x_0 = x_1 = 0$ by "$\lambda_i \neq 0, p_i \neq 0$", from the above linear relation. Similarly to the above, it occurs that "$x_0 = x_1 = x_r = 0$ for any r with $2 \leq r \leq N$". This is absurd.

Through the above argument, it has been obtained that all coefficients λ_i of the above linear relation are zeroes, and hence the row-vectors $\mathfrak{u}_i$'s $(0 \leq i \leq N-2)$ of J are linearly independent over k. Thus we get rank $J = N-1$ at any P. Therefore X is smooth.

Let g be the genus of X, and $d_1, d_2, \ldots, d_{N-1}$ be the degrees of equations defining X, respectively. Then through the known genus-formula:

$$g = 1 + \frac{1}{2} \cdot \prod_{i=1}^{N-1} d_i \cdot \left(\sum_{i=1}^{N-1} d_i - N - 1 \right)$$

(cf. Chapter IV, §2-7 in [5]), we have

$$g = 1 + \frac{1}{2}(q+1)^{N-1}\left[(N-1)q - 2\right],$$

by $d_i = q + 1 (1 \leq i \leq N-1)$.

On the other hand, let d be the degree of X and $\Gamma_{q',N}$ be the number of $\mathbb{F}_{q'}$-rational points on the curve X. In Case [A], since $\iota(q'; X) = 1$ for $q' = q^2$, we have

$$\Gamma_{q',N} = d(q'-1) - (2g-2) \quad \text{for} \quad q' = q^2,$$

through the formula of Theorem 1 in [3].

Therefore, for the curve $X \subset \mathbb{P}^N$ in Case [A] of the Theorem, it is obtained that

$$\Gamma_{q',N} = (q+1)^{N-1}\left[q^2 + 1 - (N-1)q\right] \quad \text{for} \quad q' = q^2,$$

by $d = (q+1)^{N-1}$.

References

1. A. García and M. Homma, Frobenius Order-Sequences of Curves, *in* “Proceeding of the Conference on Algebra and Number Theory held at the Institute for Experimental Mathematics, University of Essen (Germany), December 2-4, 1992”, pp. 1–15.
2. A. García and J.F. Voloch, Duality for projective curves, *Bol. Soc. Bras. Mat.* **21**(2) (1991), 159–175.
3. A. Hefez and J.F. Voloch, Frobenius non classical curves, *Arch. Math.* **54** (1990), 263–273.
4. F.K. Schmidt, Die Wronskische Determiante in beliebigen differenzierbaren Funktionenkörpern, *Math. Z.* **45** (1939), 62–74.
5. J.-P. Serre, *Groupes algébriques et corps de classes*, Actualités Sci. Ind. Hermann, 1959.
6. K.-O. Stöhr and J.F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52**(3) (1986), 1–19.